District Of Columbia (DC) – Justice Information System (JUSTIS) Security Control Requirements

11 December 2000

σ

Prepared for the:
District of Columbia (DC) Criminal Justice Coordinating Council (CJCC)

TABLE OF CONTENTS

JUSTIS SECURITY CONTROL REQUIREMENTS

1.0 INTRODUCTION

On July 19, 2000, the Criminal Justice Coordinating Council (CJCC) of the District of Columbia (DC) entered into a Purchase Order Agreement (i.e., Contract Number ATOP002647) with Mitretek Systems, Inc., (hereinafter "Mitretek") for support in the identification and documentation of the functional security requirements for DC's new Criminal Justice Information Systems Intranet (JUSTIS). Two forms of documentation are required under the contract:

1. Draft JUSTIS System Security Plan (SSP) stating all of the functional security requirements for JUSTIS in the format prescribed by the Computer Security Act of 1987 and Office of Management and Budget (OMB) Circular A-130.
2. Draft Functional Requirements Document (FRD) setting forth the technical functional security requirements for JUSTIS in the format prescribed in the life-cycle documentation requirements of the United States Department of Justice (DOJ).

On Friday, October 27, 2000, Mitretek was advised by the CJCC that neither of the two contractually-required forms of documentation fully met the CJCC's need for a more concise statement of JUSTIS security requirements. It was thereupon agreed that a third document would be developed to provide a more concise statement of the security program and control requirements that JUTIS must satisfy. This document responds to that agreement. The security program and control requirements applicable to JUSTIS are set forth herein. The source documents from which the requirements have been extracted are cited and available in the JUSTIS SSP previously submitted to the CJCC.

2.0 AUTOMATED INFORMATION SECURITY PROGRAM REQUIREMENT

Agencies must implement, document, and maintain a program to assure that adequate security is provided for all sensitive information collected, processed, transmitted, stored, or disseminated by its information systems.

3.0 SECURITY RESPONSIBILITY ASSIGNMENT REQUIREMENT

Responsibility for JUSTIS security must be assigned, in writing, to an individual(s) who is knowledgeable in the information technology used and in providing security for such technology. All security-related assignments of responsibility must be made in writing.

4.0 SYSTEM SECURITY PLAN REQUIREMENTS

A System Security Plan (SSP) must be developed and maintained for each information system operated by or on behalf of the CJCC.

5.0 MANAGEMENT CONTROL REQUIREMENTS

5.1 RISK ASSESSMENT AND MANAGEMENT

A risk-based approach must be used to determine and justify specific security control requirements, which requires risk assessment.

5.1.1 Risk Assessment

Risk assessment must be used to support two related functions: the acceptance of risk and the selection of cost-effective controls.

Risk assessment must be conducted before putting the system into operation in a production environment and immediately following any significant change to the information system. Risk assessment must also be conducted not less than once every 3 years.

Risk assessment, the process of analyzing and interpreting risk, is comprised of three basic activities: (1) determining the assessment's scope and methodology; (2) collecting and analyzing data; and (3) interpreting the risk analysis results." The general step-by-step requirements for a risk assessment are set forth below.

5.1.1.1 Asset Valuation

Proper risk assessment requires asset valuation. Assets include information, software, personnel, hardware, and physical assets (such as the computer facility). The value of an asset consists of its intrinsic value and the near-term impacts and long-term consequences of its compromise.

5.1.1.2 Consequence Assessment

The consequence assessment estimates the degree of harm or loss that could occur. Consequences refer to the overall aggregate harm that occurs, not just to the near-term or immediate impacts. The more severe the consequences of a threat, the greater the risk to the system (and therefore, the organization).

5.1.1.3 Threat Analysis

A threat is an entity or event with the potential to harm the system. Threats must be identified and analyzed to determine the likelihood of their occurrence and their potential to harm assets.

5.1.1.4 Safeguard Analysis

A safeguard is any action, device, procedure, technique, or other measure that reduces a system's vulnerability to a threat. Safeguard analysis must include an examination of the effectiveness of the existing security measures.

5.1.1.5 Vulnerability Assessment

A vulnerability is a condition or weakness in, or absence of, security procedures, technical controls, physical controls, or other controls that could be exploited by a threat. Vulnerabilities are analyzed in terms of missing safeguards. Vulnerabilities contribute to risk because they "allow" a threat to harm the system.

5.1.1.6 Likelihood Assessment

Likelihood is an estimation of the frequency or chance of a threat happening. A likelihood assessment considers the presence, tenacity, and strengths of threats as well as the effectiveness of safeguards (or presence of vulnerabilities). In general, the greater the likelihood of a threat occurring, the greater the risk."

5.1.1.7 Uncertainty Analysis

Uncertainty Analysis. Risk management often must rely on speculation, best guesses, incomplete data, and many unproven assumptions. The uncertainty analysis attempts to document this so that the risk management results can be used knowledgeably. There are two primary sources of uncertainty in the risk management process: (1) lack of confidence or precision in the risk management model or methodology, and (2) lack of sufficient information to determine the exact value of the elements of the risk model, such as threat frequency, safeguard effectiveness, or consequences.

5.1.2 Risk Mitigation

Risk mitigation involves the selection and implementation of security controls to reduce risk to a level acceptable to management, within acceptable constraints. The selection of safeguards and risk acceptance testing are likely to be performed simultaneously. This is often viewed as a circular, iterative process.

5.1.2.1 Select Safeguards

A primary function of security risk management is the identification of appropriate controls. One method of selecting safeguards uses a "what if" analysis. With this method, the effect of adding various safeguards (and therefore, reducing vulnerabilities) is tested to see what difference each makes with regard to cost, effectiveness, and other relevant factors. Trade-offs among the factors can be seen. The analysis of trade-offs also supports the acceptance of residual risk. Another method is to categorize types of safeguards and recommend implementing them for various levels of risk. As with other aspects of risk management, the actual safeguards selected for implementation should concentrate on the highest risk areas.

5.1.2.2 Accept Residual Risks

At some point, management must decide if the operation of the information system is acceptable, given the kind and severity of remaining risks. One of the two primary functions of risk management is the interpretation of risk for the purpose of risk acceptance.

5.2 REVIEW OF SECURITY CONTROLS

The security controls in each system must be reviewed when significant modifications are made to the system, but at least every three years. The scope and frequency of the review should be commensurate with the acceptable level of risk for the system. Reviews should assure that management, operational, personnel, and technical controls are functioning effectively.

5.3 RULES OF THE SYSTEM

Each agency that maintains a system of records covered by the Privacy Act of 1974 must establish rules of conduct for persons involved in the design, development, operation, or maintenance of that system of records, and must instruct each such person with respect to such rules and the penalties for non-compliance. The rules shall be based on the needs of the various users of the system. The security required by the rules shall be only as stringent as necessary to provide adequate security for the information in the system. Such rules shall clearly delineate responsibilities and expected behavior of all individuals with access to the system. They shall also include appropriate limits on interconnections to other systems and shall define service provision and restoration priorities. The rules must be in writing and form the basis for security awareness and training.

5.4 PLANNING FOR SECURITY IN THE LIFE CYCLE

Security must be managed throughout a system's life cycle. This specifically includes ensuring that changes to the system are made with attention to security and that accreditation is accomplished.

5.4.1 Initiation Phase

The conceptual and early design process of a system involves the discovery of a need for a new system or enhancement to an existing system; early ideas as to system characteristics and proposed functionality; brainstorming sessions on architectural, performance, or functional system aspects; and environmental, financial, political, or other constraints. At the same time, the basic security aspects of a system must be developed and documented along with early system design. This can be done through a sensitivity assessment.

5.4.2 Development/Acquisition Phase

During this phase, the system is designed, purchased, programmed, developed, or otherwise constructed. Security requirements must be developed and documented at the same time system planners define the requirements of the system. These requirements can be expressed as technical features (e.g., access controls), assurances (e.g., background checks for system developers), or operational practices (e.g., awareness and training).

5.4.3 Implementation Phase

During implementation, the system is tested and installed or fielded. The system's security features must be configured and enabled during this phase. A design review and system test must be performed prior to placing the system into operation to assure that it meets security specifications. In addition, if new controls are added, additional acceptance tests of those new controls must be performed. This ensures that the new controls meet security specifications and do not conflict with or invalidate existing controls.

5.4.4 Operational Phase

During the Operational Phase, the system performs its work. The system is almost always being continuously modified by the addition of hardware and software and by numerous other events. The system is undergoing modifications. Many security activities take place during the Operational Phase of a system's life. In general, they fall into three areas: (1) security operations and administration; (2) operational assurance; and (3) periodic re-analysis of the security.

5.4.5 Disposal Phase

The Disposal Phase of the system's life cycle involves the disposition of information, hardware, and software.

5.5 SYSTEM CERTIFICATION AND ACCREDITATION

JUSTIS must undergo security certification and accreditation (C&A) prior to being permitted to operate in a production environment, immediately following any significant change, or not less than once every three years.

The principal purpose of the security certification and accreditation process is to protect the entities comprising the information infrastructure with a proper balance between the benefits to the operational missions, the risks to those same missions, and the life cycle costs.

C&A should be conducted in the following phases.

5.5.1 Phase I Definition

The Definition Phase includes activities to verify the system mission environment and architecture, identify the threat, define the levels of effort, identify the Designated Approving Authority and Certification Authority (Certifier), and document the C&A security requirements.

5.5.1.1 Collect Information and Documentation About the System

During the preparation activity, information and documentation is collected about the system. This information includes capabilities and functions the system will perform, desired interfaces and data flows associated with those interfaces, information to be processed, operational organizations supported, intended operational environment, and operational threats. Typically, this information is contained in the business case or mission needs statement, system specifications, architecture and design documents, user manuals, operation procedures, network diagrams, and configuration management documentation, if available. National, agency, and organizational level security instructions and policies should also be reviewed.

5.5.1.2 Registration

Registration initiates the risk management agreement process. Information is evaluated, applicable information assurance requirements are determined, risk management and vulnerability assessment actions begin, and the level of effort required for C&A is determined and planned.

5.5.1.3 Negotiation

During Negotiation all participants involved in the information system's development, acquisition, operation, security certification, and accreditation reach agreement on the implementation strategy to be used to satisfy the security requirement identified during system registration. The negotiation tasks are, conduct the certification requirements review (CRR), agreement on the security requirements, level of effort, and schedule, and approve final Phase I System Security Accreditation Agreement (SSAA).

5.5.2 Phase II Verification

The Verification Phase includes activities to document compliance of the system with previously agreed on security requirements. For each life cycle development activity, there is a corresponding set of security activities that verifies compliance with the security requirements and constraints and evaluates vulnerabilities. Phase 2 activities include verifying security requirements during system development or modification, certification analysis, Certification Testing and Evaluation (CT&E), and analysis of the certification results.

5.5.2.1 SSAA Refinement

Phase 2 starts with a review of the SSAA. If there has been a significant time delay since the completion of Phase 1 or if new people are involved in the C&A process, the SSAA should be reviewed in detail.

5.5.2.2 System Development and Integration

System development and integration activities are those activities required for development or integration of the information system components as defined in the system's functional and security requirements. This activity verifies that the requirements in the SSAA are met in the evolving system before it is integrated into the operating environment.

5.5.2.3 Initial Certification Analysis

The initial certification analysis determines if the information system is ready to be evaluated and tested during Phase 3, Validation. Initial certification analysis verifies that the development, modification, and integration efforts will result in a higher probability of success for an accreditable information system before Phase 3 begins. Certification tasks are tailored to the system development activities to ensure conformance with the SSAA.

5.5.2.4 Assess Analysis Results

At the conclusion of each development or integration milestone, the certification analysis results are reviewed. If the results indicate significant deviation from the SSAA, the C&A should return to Phase 1 to resolve the problems. If the results are acceptable, the C&A proceeds to the next task or to Phase 3.

5.5.3 Phase III Validation

Phase 3 certification tasks include certification of software, firmware, hardware, and inspections of operational sites to ensure their compliance with physical security, procedural security, TEMPEST (i.e., prevention of electromagnetic emissions) and communications security (COMSEC) requirements, personnel security, and security education, training, and awareness requirements.

5.5.3.1 SSAA Refinement

Phase 3 includes tasks to certify the compatibility of the computing environment with the description provided in the SSAA.

5.5.3.2 Certification Evaluation of Integrated System

This activity certifies that the fully integrated and operational system will comply with the requirements stated in the SSAA and the system will be operated with an acceptable level of residual risk. During this activity, certification tasks are preformed to ensure that the information system is functionally ready for operations. The certification tasks and the extent of the tasks will depend on the level of certification analysis in the SSAA.

5.5.3.3 Recommendation to Accreditor

The purposes of this activity are to consolidate the findings developed during certification of the integrated system and submit the Certifier's report to the DAA. If the Certifier concludes that the integrated information system satisfies the SSAA technical requirements, the Certifier issues a system certification. The system certification certifies that the information system has complied with the documented security requirements. Supplemental recommendations might also be made to improve the system's security posture.

5.5.3.4 Accreditation Decision

After receipt of the Certifier's recommendation, the DAA reviews the SSAA and makes an accreditation determination. This determination is added to the SSAA. The final SSAA accreditation package includes the Certifier's recommendation, the DAA authorization to

operate, and supporting documentation. If the decision is to accredit, the decision must include the security parameters under which the information system is authorized to operate. If the system does not meet the requirements stated in the SSAA, but mission criticality mandates that the system become operational, an Interim Approval to Operate (IATO) may be issued.

5.5.4 Phase IV Post Accreditation

Post accreditation activities include ongoing maintenance of the SSAA, system operations, security operations, configuration management, and compliance validation.

5.5.4.1 System and Security Operation

The system operation activity includes the secure operations of the information system and the associated computing environment. System maintenance tasks ensure that the information system continues to operate within the stated parameters of the accreditation.

5.5.4.2 Compliance Validation

The purpose of this activity is to ensure the system continues to comply with the security requirements, current threat assessment, and the concept of operations. The compliance review should ensure that the contents of the SSAA adequately address the functional environment into which the information system has been placed. The compliance validation tasks should repeat all the applicable Phase 2 and 3 tasks.

5.6 AUTHORIZE PROCESSING

Management authorization to process in the production mode should be based on an assessment of management, operational, and technical controls. Since the security plan establishes the security controls, it should form the basis for the authorization, supplemented by more specific studies as needed. In addition, the periodic review of controls should also contribute to future authorizations. Some agencies perform "certification reviews" of their systems periodically. These formal technical evaluations lead to a management accreditation, or "authorization to process." Re-authorization must occur prior to a significant change in processing, but at least every three years. It should be done more often where there is a high risk and/or potentially high magnitude of harm.

6.0 OPERATIONAL CONTROLS

The greatest harm/disruption to a system comes from the actions of individuals, both intentional and unintentional. All too often, systems experience disruptions, damage, loss, or

other adverse impact due to the well-intentioned actions of individuals authorized to use or maintain a system.

6.1 PERSONNEL SECURITY

Every general support system includes a number of technical, operational, and management controls that are used to prevent and detect harm. Such controls include individual accountability, "least privilege," and "separation of duties."

6.1.1 Access Authorization

No information system can be secured without properly addressing how users, designers, implementers, and managers interact with computers, individuals, and the access and authorities they need to do their jobs. The CJCC must make clear designations regarding who may authorize access to their information systems.

6.1.2 Limited Access

Direct access to criminal history record information shall be available only to authorized officers or employees of a criminal justice agency and, as necessary, other authorized personnel essential to the proper operation of the criminal history record information system.

6.1.2.1 Position Sensitivity Analysis

The responsible manager shall determine the position's sensitivity based on the duties and access levels, so that appropriate cost-effective screening can be completed.

6.1.2.2 Background Screening

Once a position's sensitivity has been determined, the position is ready to be staffed. More sensitive positions typically require pre-employment background screening; screening after employment has commenced (post entry-on-duty) may suffice for less sensitive positions, however, good management practices dictate record checks should be completed prior to employment.

6.1.2.3 Limitations on Access Prior to Background Screening

If individuals are permitted system access prior to completion of appropriate background screening, the conditions under which this is allowed and any compensating controls to mitigate the associated risk must be especially approved during the C&A process.

6.1.2.4 Application of the Principle of Least Privilege

Once a position has been broadly defined, the responsible supervisor shall determine the type of computer access needed for the position. Least privilege refers to the security objective of granting users only those accesses they need to perform their official duties.

6.1.2.5 Application of the Principle of Separation of Duties

Separation of duties refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process.

6.1.2.6 User Administration

Effective administration of users' computer access is essential to maintaining system security. User account management focuses on identification, authentication, and access authorizations; auditing and otherwise periodically verifying the legitimacy of current accounts and access authorizations; and timely modifications or removal of access and associated issues for employees who are reassigned, or terminated, or who retire.

6.1.3 Individual Accountability

Mechanisms must be put in place for holding users individually responsible for their actions.

6.1.4 Facility Identification Badges

Mechanisms must be put in place for issuing and controlling employee and visitor facility identification badges, which must be worn by all personnel in the facility housing the information system.

6.1.4.1 Employee Badges

Stringent methods of control over employee badges will ensure that employees wearing badges have been screened and are authorized to be at the facility during the appropriate time frame.

6.1.4.2 Visitor Badges

Stringent methods of control over visitor badges will ensure that visitors wearing badges have been screened and are authorized to be at the facility during the appropriate time frame.

6.1.5 Visitors in Controlled Areas

All visitors to computer centers and/or terminal areas must be accompanied by authorized staff personnel at all times.

6.1.6 Termination/Debriefing

Termination of a user's system access generally can be characterized as either "friendly" or "unfriendly." Friendly terminations shall be accomplished by implementation of a standard set of procedures for outgoing or transferred employees. This normally includes: removal of access procedures, computer accounts, authentication tokens; the control of keys; the briefing on the continuing responsibilities for confidentiality and privacy; return of property; and continued availability of data. In the case of unfriendly termination, given the potential for adverse consequences, organizations shall do the following: system access should be terminated as quickly as possible; and in some cases, physical removal from the office may be necessary.

6.2 PHYSICAL AND ENVIRONMENTAL PROTECTION

Physical and environmental security controls must be implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. All organization's physical and environmental security programs should address the following seven topics (access controls, fire safety, failure of supporting utilities, structural collapse, plumbing leaks, interception of data, and mobile and portable systems).

6.3 PRODUCTION, INPUT/OUTPUT (I/O) CONTROLS

Controls must be established for the marking, handling, processing, storage, and disposal of input and output information and media, as well as labeling and distribution procedures for the information and media.

6.4 CONTINGENCY PLANNING

Establish and periodically test the capability to continue providing service within a system based upon the needs and priorities of the participants of the system.

6.5 HARDWARE AND SYSTEM SOFTWARE MAINTENANCE CONTROLS

These controls are used to monitor the installation of, and updates to, hardware, operating system software, and other software to ensure that the hardware and software function as expected, and that a historical record is maintained of application changes. These controls may also be used to ensure that only authorized software is installed on the system.

6.6 INTEGRITY CONTROLS

Integrity controls are used to protect the operating system, applications, and information in the system from accidental or malicious alteration or destruction and to provide assurance to the user that the information meets expectations about its quality and that it has not been altered.

6.7 DOCUMENTATION

Documentation of all aspects of computer support and operations is important to ensure continuity and consistency. Formalizing operational practices and procedures with sufficient detail helps to eliminate security lapses and oversights, gives new personnel sufficiently detailed instructions, and provides a quality assurance function to help ensure that operations will be performed correctly and efficiently. The security of a system also needs to be documented. This includes many types of documentation, such as security plans, contingency plans, risk analyses, and security policies and procedures. Much of this information, particularly risk and threat analyses has to be protected against unauthorized disclosure. Security documentation also needs to be both current and accessible.

6.8 SECURITY AWARENESS AND TRAINING

Mandatory periodic training is required for all persons involved in management, use, or operation of information systems that contain sensitive information.

7.0 TECHNICAL CONTROLS

Technical controls focus on security controls that the information system executes. The controls can provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. The implementation of technical controls, however, always requires significant operational considerations and should be consistent with the management of security within the organization.

7.1 IDENTIFICATION AND AUTHENTICATION

Identification and Authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an information system. Access control usually requires that the system be able to identify and differentiate among users. User accountability requires the linking of activities on an information system to specific individuals and therefore requires the system to identify users.

7.1.1 Identification

Identification is the means by which a user provides a claimed identity to the system. The most common form of identification is the user ID.

7.1.1.1 Unique Identification

An organization shall require users to identify themselves uniquely before being allowed to perform any actions on the system.

7.1.1.2 Correlate Actions to Users

The system shall internally maintain the identity of all active users and be able to link actions to specific user.

7.1.1.3 Maintenance of User IDs

The organization should ensure that all user IDs belong to currently authorized users. Identification data must be kept current by adding new users and deleting former ones.

7.1.1.4 Inactive User IDs

When user accounts are no longer required, the accounts shall be removed in a timely manner. User IDs that are inactive on the system for a specific period of time (e.g., three months) should be disabled.

7.1.2 Authentication

Authentication is the means of establishing the validity of a user's claimed identity to the system. There are three means of authenticating a user's identity, which can be used alone or in combination: something the individual knows; something the individual possesses; and something the individual is.

7.2 AUDIT TRAILS

Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification.

7.3 INTRUSION DETECTION

Intrusion detection refers to the process of identifying attempts to penetrate a system and gain unauthorized access. If audit trails have been designed and implemented to record appropriate information, they can assist in intrusion detection. Although normally thought of as a real-time effort, intrusion can be detected in real time by examining audit records as they are created or after the fact

7.4. REVIEW PROCEDURES

Audit trails shall be reviewed periodically. The following should be considered when reviewing audit trails: recognize normal activity, contain a search capability, follow-up reviews, develop review guidelines, and automated tools. Keystroke monitoring is a process used to view or record both the keystrokes entered by a computer user and the computer's response during an interactive session. Keystroke monitoring is usually considered a special case of audit trails. The Department of Justice has advised that an ambiguity in the U.S. law makes it unclear whether keystroke monitoring is considered equivalent to an unauthorized telephone wiretap. If keystroke monitoring is used in audit trails, organizations should have a written policy and notify users.

7.5 LOGICAL ACCESS CONTROLS

Logical access controls are the system-based mechanisms used to specify who or what (e.g., in the case of a process) is to have access to a specific system resource and the type of access that is permitted.

7.6 WARNING BANNERS

Public Law 99-474 requires that a warning message be displayed, notifying unauthorized users that they have accessed a government computer system and unauthorized use can be punished by fines or imprisonment. Prior to user authentication, the system should display a banner warning that use of the system is restricted to authorized personnel.